



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/830,127	04/22/2004	Paul A. Gassoway	063170.6962	7446
5073	7590	08/22/2008		
BAKER BOTTS L.L.P.			EXAMINER	
2001 ROSS AVENUE				TRAORE, FATOUMATA
SUITE 600			ART UNIT	PAPER NUMBER
DALLAS, TX 75201-2980			2136	
			NOTIFICATION DATE	DELIVERY MODE
			08/22/2008	ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com  
glenda.orrantia@bakerbotts.com

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>
	10/830,127	GASSOWAY, PAUL A.
	<b>Examiner</b>	<b>Art Unit</b>
	FATOUMATA TRAORE	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 15 May 2008.  
 2a) This action is **FINAL**.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-5,7-10,12-21,23-2, 28-37, 39-42, 44-60 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-5,7-10,12-21,23,28-37,39-42 and 44-60 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) <input type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____ .
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____ .	5) <input type="checkbox"/> Notice of Informal Patent Application
	6) <input type="checkbox"/> Other: _____ .

## **DETAILED ACTION**

1. This is in response to the amendment filed on November 11<sup>th</sup>, 2007. Claims 1, 7, 8, 10, 12-15, 17, 23, 24, 26, 28-31, 33, 39, 40, 42 and 44-47 have been amended; Claims 49-60 have been added; Claims 6, 11, 22, 27, 38 and 43 have been cancelled; Claims 1-5, 7-10, 12-21, 23-26, 28-37, 39-42 and 44-60 are pending in this application and have been considered below.

### ***Response to Arguments***

2. On page 14 of the response Applicant argued that Arnold teaches “known undesirable software”, but fails to teach “database of unfamiliar software”. The examiner respectfully disagrees with Applicant’s interpretation of the Arnold teaching. Contrary to Applicant’s assertion, Arnold teaches detecting the presence of an undesirable software entity (e.g., virus, worm, Trojan horse)> See abstract. As depicted in Fig. 2(items B and C), Arnold teaches both “know software” and “unknown software.”

3. Applicant also argued that Arnold fails to teach “the entry has been in the database of unfamiliar software for a sufficient period of time “. The examiner respectfully disagrees. In Fig. 3, Arnold discloses run the checkup periodically (B). The “periodically checking is set for a “sufficient period of time”. In fact, Arnold discloses performing the “checkup” for “a specified time interval”. See column 6, lines 24-36. In addition, Arnold discloses” moving the entry” to a [know] database. See Fig. 3.

4. Applicant further argues that McGee fails to teach “a database of unfamiliar software”. Applicant contends that “Verna fails to cure the deficiencies”. The examiner

notes that the previous Office action failed to use the proper combination of references to reject the claims, in particular claim 56. To clarify the rejection, the proper combination of references is now being used. Claim 56 is now rejected over McGee, Verna and Arnold.

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-5, 12-21, 28-37 and 44-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over McGee et al (US 6,694,434) in view of Arnold et al (US 5,440,723).

***Claims 1, 17 and 33:*** McGee et al discloses a method, a system, and a computer recording medium for controlling program execution and program distribution comprising:

Providing a database of known good software (application registration data is a list of hash value of approved application) (column 5, lines 13-32; fig .5, item 500);

Opening a file (if an executable file open commencement request is detected) (column 11, lines 3-35; Fig. 5, item 508);

Identifying the file being opened (the processor retrieves file filter criteria as shown in block 510. File filter criteria include any suitable data identifier) (column 11, lines 3-35);

Determining whether an entry exists in the database of known good software for the identified file (As shown in block 516, the node uses its hash value generator to generate a hash of the program designated for execution and compares the generated hash value with the stored hash values on the approved hash list. This is shown in block 518. If the generated hash value appears on the approved hash list, the processor grants executability to the program designated for execution as shown in block 520) (column 11, line 37 to column 12 line 4);

Determining whether an entry exists in the database of unfamiliar software for the identified file (As shown in block 516, the node uses its hash value generator to generate a hash of the program designated for execution and compares the generated hash value with the stored hash values on the approved hash list. This is shown in block 518. If the generated hash value appears on the approved hash list, the processor grants executability to the program designated for execution as shown in block 520) (column 11, line 37 to column 12 line 4);

Performing at least one of allowing and preventing the opening of the file from continuing based on the result of the determination (As such, the process may occur in fore ground or background operation and prevents

an executable program from being run if it does not appear on the approved hash list. As shown in block 522, if the hash value generated by the receiving processor does not match the hash value on the approved hash list, the system prevents the executable file data from executing and may optionally record the non-approval condition based on the comparison, log the event and/or inform the user) (column 11, line 37 to column 12 line 4).

But does not explicitly disclose a step of provide providing a database of unfamiliar software nor the step of Moving the entry from the database of unfamiliar software to the database of known good software if it is determined that the entry has been in the database of unfamiliar software for a sufficient period of time. However, Arnold et al discloses an automatic immune method, system, and computer recording medium for computers, which further discloses:

Providing a database of unfamiliar software (column 29, lines 18-25);  
Moving the entry from the database of unfamiliar software to the database of known good software if it is determined that the entry has been in the database of unfamiliar software for a sufficient period of time (Fig. 2, item step E; Fig.3, step O).

Therefore, it would be obvious to one having ordinary skills in the art at the time the invention was made to provide a database of unfamiliar software in McGee et al's disclosure. One would have been motivated to provide such a database in

order to maintain the integrity of the system by not allowing malicious code to be executed.

**Claims 2, 18, 34:** McGee et al and Arnold et al disclose a method, a system, and a computer recording medium for controlling program execution and program distribution as in claims 1, 17, and 33 above, and McGee et al further discloses that the file comprises an executable file (The system may compare a location of the executable file data with the location of approved executable file data indicated by the application registration data in the list) (column 4, lines 7-11, column 8, lines 60-65).

**Claims 3, 19, 35:** McGee et al and Arnold et al disclose a method, a system, and a computer recording medium for controlling program execution and program distribution as in claims 2, 18, and 34 above, and McGee et al further discloses the executable file comprises an application (the application registration data contains a plurality of first unique application verification) (column 3 line 64 to column 4 line 4).

**Claims 4, 20, 36:** McGee et al and Arnold et al disclose a method, a system, and a computer recording medium for controlling program execution and program distribution as in claims 1, 17, and 33 above, and McGee et al further discloses that the step of identifying the file being opened comprises determining a unique value of the file, the unique value being a hash value generated according to a hashing algorithm and comparing the unique value to entries in the database of known good software (an approved stored list of hash values for approved

executable files for programs, for example, is generated by a trusted party. Prior to allowing individual program execution by the first-party, the first-party generates or retrieves a second unique application verification data element, such as a hash value, of an executable file designated for execution on a processing device, such as a computer or the communication unit. The stored hash values from the list are evaluated and compared to the generated hash value. The first-party system grants program executability on a per-program basis based on the comparison of the pre-stored hash values and hash value generated by the party having the program designated for execution)(column 4, lines 5-35).

**Claims 5, 21, 37:** McGee et al and Arnold et al disclose a method, a system, and a computer recording medium for controlling program execution and program distribution as in claims 4, 20, and 36 above, and McGee et al further discloses that the step of the performing at least one of allowing and preventing the opening of the file from continuing comprises allowing the file to continue to be opened if it is determined that the determined unique value corresponds to an entry in the database of known good software (As such, the process may occur in fore ground or background operation and prevents an executable program from being run if it does not appear on the approved hash list. As shown in block 522, if the hash value generated by the receiving processor does not match the hash value on the approved hash list, the system prevents the executable file data from executing and may optionally record the non-approval condition based

on the comparison, log the event and/or inform the user) (column 11, line 37 to column 12 line 4).

**Claims 12, 28, 44:** McGee et al and Arnold et al disclose a method, a system, and a computer recording medium for controlling program execution and program distribution as in claims 6, 22, and 38 above, and McGee et al further discloses a step of adding an entry to the database of unfamiliar software if an entry for the file being opened is not found in at least one of the database for known good software and the database for unfamiliar software (the trusted authority selects the candidate programs that, for example, are to be passed through a hash function and made part of the approved hash list. The central authority may obtain this information by entry through a graphic user interface by a system administrator or may have the information automatically downloaded from another source) (column 12, lines 19-63).

**Claims 13, 29, 45:** McGee et al and Arnold et al disclose a method, a system, and a computer recording medium for controlling program execution and program distribution as in claims 6, 22, and 38 above, and McGee et al further discloses a step of placing at least one operating system call hook if it is determined that an entry exists in the database for unfamiliar software (a matching of hash values based on the entire executable file from a list of approved hash values results in the calling application being granted access to execute) (column 13, lines 30-38).

**Claims 14, 30, 46:** McGee et al and Arnold et al disclose a method, a system, and a computer recording medium for controlling program execution and program distribution as in claims 13, 29, and 45 above, and McGee et al further discloses that the operating system call hook notifies a Trojan notification service that a file corresponds to an entry in the database for unfamiliar software (If the computed unique application verification data does not match the stored unique application verification data, the user is notified that the application is listed in the application registration but may have been upgraded or it is an unauthorized application as indicated in block 74) (column 8, lines 16-22).

**Claims 15, 31, 47:** McGee et al and Arnold et al disclose a method, a system, and a computer recording medium for controlling program execution and program distribution as in claims 14, 30, and 46 above, and McGee et al further discloses that the Trojan notification service prompts a user for input regarding whether the operating system call should be passed along (The system then generates a signal (for example, resulting in a prompt to the user) (column 8, lines 25-30).

**Claims 16, 32, 48:** McGee et al and Arnold et al disclose a method, a system, and a computer recording medium for controlling program execution and program distribution as in claims 15, 31, and 47 above, and McGee et al further discloses that the step of opening of the file is allowed to proceed if the operating system call is passed along (The user is then prompted to indicate whether execution privileges should be granted to the application as shown in block 86.

This may be done, for example, through a graphic user interface. If the user responds indicating that execution privileges should be granted, the application is then added to the application registration list as shown in block 88) (column 8, lines 41-65).

7. Claims 7, 23, 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over McGee et al (US 6,694,434) in view of Arnold et al (US 5,440,723) and further in view of Liu et al (US 6,760,752).

**Claims 7, 23, and 39:** McGee et al and Arnold et al disclose a method, a system, and a computer-recording medium for controlling program execution and program distribution as in claims 6, 22, and 38 above, while neither of them explicitly disclose a step of providing a time stamp. However, Liu et al discloses a method, a system and a computer recording medium for securely transferring a message from a sender to a receiver, which further discloses a step of providing date stamp information for each entry in the database for unfamiliar processes indicating a date on which the entry was first made (a time stamp process and a status retrieval process) (column 25 line 57 to column 26 line 45, Figs. 2 B item 262, 8 A and 8B). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method, system, and computer recording medium of McGee et al and Arnold et al such as to provide a time stamp information for each entry. The motivation of doing so would have been to ensure the integrity of information sent over a network.

8. Claims 10, 26 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over McGee et al (US 6,694,434) and of Arnold et al (US 5,440,723) in view of Liu et al (US 6,760,752) and further in view of Verma (US 7,140,042).

**Claims 10, 26, 42:** McGee et al, Arnold et al, and Liu et al disclose a method, a system, and a computer-recording medium for controlling program execution and program distribution as in claims 7, 23, and 39 above, while neither of them explicitly discloses a step of determining the amount of time. However, Verma discloses a method, a system and a computer recording medium preventing software piracy, which further discloses a step of determining an amount of time an entry has been in the database for unfamiliar processes by comparing the date stamp information with a current date (column 5, lines 8-20). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method, system, and computer-recording medium of McGee et al, Arnold et al, and Liu et al such as to determine a time limit. The motivation of doing so would have been to keep in track of the usage of the application.

9. Claims 8-9, 24-25, 40-41, 49, 51 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over McGee et al (US 6,694,434) in view of Arnold et al (US 5,440,723) and further in view of Verma (US 7,140,042).

**Claims 8, 24, 40:** McGee et al and Arnold et al disclose a method, a system, and a computer recording medium for controlling program execution and program distribution as in claims 1, 17, and 33 above, while neither of them explicitly discloses a step of providing a number of times corresponding to the opening of an entry. However, Verma discloses a method, a system and a computer recording medium preventing software piracy, which further discloses a step of providing a value for each entry in the database for unfamiliar software indicating a number of times a file corresponding to the entry was opened (column 11, lines 44-57). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method, system, and computer-recording medium of McGee et al and Arnold et al such as to provide the number of time the was opened. The motivation of doing so would have been to keep in track of the usage of the application.

**Claims 9, 25, 41:** McGee et al, Arnold et al and Verma disclose a method, a system, and a computer recording medium for controlling program execution and program distribution as in claims 8, 24, and 40 above, while neither of them explicitly discloses a step of providing a number of times a file has been executed. However, Verma discloses a method, a system and a computer-recording medium preventing software piracy, which further discloses a step of providing a value comprises the number of times an executable in file has been executed (column 11, lines 44-57). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the

combined method, system, and computer-recording medium of McGee et al and Arnold et al such as to determine the number of time a file has been executed.

The motivation of doing so would have been to keep in track of the usage of the application.

**Claims 49, 51, 54:** McGee et al, Arnold et al and Verma disclose a method, a system, and a computer recording medium for controlling program execution and program distribution as in claims 8, 24, and 40 above, while neither of them explicitly discloses a step of providing a number of times a file has been executed. However, Verma discloses a method, a system and a computer-recording medium preventing software piracy, which further discloses a step of providing a value comprises the number of times an executable in file has been executed (column 11, lines 44-57). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method, system, and computer-recording medium of McGee et al and Arnold et al such as to determine the number of time a file has been executed. The motivation of doing so would have been to keep in track of the usage of the application.

10. Claims 56-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over McGee et al (US 6,694,434) in view of Verma (US 7,140,042) in further view of Arnold et al (US 5,440,723).

***Claim 56:*** McGee et al discloses a method for controlling program execution and program distribution comprising:

- i. Identifying a file (column 11, lines 3-35);
- ii. Determining whether an entry for the file exists in database of unfamiliar software (column 11, line 37 to column 12 line 4);
- iii. Adding an entry for the file to a database of known good software if the quantitative information exceeds a predetermined value( Fig. 5); and
- iv. Allowing the opening of the file to continue if the database of known good software includes the entry for the file (column 11, line 37 to column 12 line 4).

But does not explicitly disclose the step of Determining quantitative information regarding the file, the quantitative information selected from the group consisting of a length of time the entry has been in the database of unfamiliar software, a number of times the file has been opened, and a number of times an executable in the file has been executed; However, Verma discloses a method, a system and a computer-recording medium preventing software piracy, which further discloses a step of determining quantitative information regarding the file, the quantitative information selected from the group consisting of a length of time the entry has been in the database of unfamiliar software (column 5, lines 8-20), a number of times the file has been opened (column 11, lines 44-57), and a number of times an executable in the file has been executed (column 11, lines 44-57).

Therefore, it would be obvious to one having ordinary skills in the art at the time the invention was made to determine quantitative information in McGee et al's disclosure. One would have been motivated to determine such information in order to maintain the integrity of the system by not allowing malicious code to be executed.

**Claim 57:** McGee et al and Verma disclose a method for controlling program execution and program distribution as in claim 56 above, while neither of them explicitly discloses a step of removing the entry for the file from the database of unfamiliar software if the quantitative information exceeds a predetermined value. However, Arnold et al discloses an automatic immune method, system, and computer recording medium for computers, which further discloses a step of removing the entry for the file from the database of unfamiliar software if the quantitative information exceeds a predetermined value (column 23, line57-61; column 26, lines 50-58). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method, system, and computer-recording medium of McGee et al and Verma such as to include new virus in the virus signature database. The motivation of doing so would have been to provide computational integrity for digital data processors and networks thereof as taught by Arnold et al (column1, lines 7-13).

**Claim 58:** McGee et al and Verma disclose a method for controlling program execution and program distribution as in claim 56 above, while neither of them explicitly discloses a step of comprising preventing the opening of the file to

continue if: the database of known good software does not include the entry for the file nor that the file attempts a suspicious activity. However, Arnold et al discloses an automatic immune method, system, and computer recording medium for computers, which further discloses comprising preventing the opening of the file to continue if:

The database of known good software does not include the entry for the file (column 25, lines 17-30); and

The file attempts a suspicious activity (column 21, lines 10-30).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method, system, and computer-recording medium of McGee et al and Verma such as to prevent opening of file in a non secure environment. The motivation of doing so would have been to provide computational integrity for digital data processors and networks thereof as taught by Arnold et al (column 1, lines 7-13).

**Claim 59:** McGee et al, Verma and Arnold et al disclose a method for controlling program execution and program distribution as in claim 58 above, and Arnold et al further discloses wherein a suspicious activity comprises updating a registry (column 21, lines 10-30). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method, system, and computer-recording medium of McGee et al and Verma such as to identify the suspicious activity. The motivation of doing so

would have been to provide computational integrity for digital data processors and networks thereof as taught by Arnold et al (column1, lines 7-13).

**Claim 60:** McGee et al, Verma and Arnold et al disclose a method for controlling program execution and program distribution as in claim 58 above, and Arnold et al further discloses wherein a suspicious activity comprises opening a second file (column 21, lines 10-30). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method, system, and computer-recording medium of McGee et al and Verma such as to prevent opening of file in a non secure environment. The motivation of doing so would have been to provide computational integrity for digital data processors and networks thereof as taught by Arnold et al (column1, lines 7-13).

11. Claims 50, 52 and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over McGee et al (US 6694434) in view of Arnold et al (US 5,440,723) and Verma (US 7,140,042) in further view of Christenson et al (US 6,324,620)..

**Claims 50, 52 and 55:** McGee et al, Verma and Arnold et al disclose a method, a system, and a computer recording medium for controlling program execution and program distribution as in claim 58 above, while neither of them explicitly discloses a step of moving the entry from the database of unfamiliar software to the database of known good software if the number of times the file corresponding to the entry was opened is greater than a baseline value.

However, Christenson et al discloses a dynamic data management based on access frequency, which further discloses moving the entry from the database of unfamiliar software to the database of known good software if the number of times the file corresponding to the entry was opened is greater than a baseline value(column 2, line 50 to column 3, line 20). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method, system, and computer-recording medium of McGee et al and Verma such as move data between databases. The motivation of doing so would have been to increase system speed and efficiency as taught by Christenson et al (column 2, lines 35-40).

### **Conclusion**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

Ft

Monday, August 18, 2008

/Brandon S Hoffman/

Primary Examiner, Art Unit 2136